日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出願年月日
Date of Application: １９９９年　１月２５日

出願番号
Application Number: 平成１１年特許願第０１６２５７号

出願人
Applicant (s): 村田機械株式会社
辻井　重男
笠原　正雄

１９９９年　８月１８日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

【書類名】　特許願
【整理番号】　19948
【提出日】　平成11年 1月25日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/14
H04L 9/30
G09C 1/00
【発明の名称】　秘密鍵生成方法，暗号化方法及び暗号通信方法
【請求項の数】　3
【発明者】
【住所又は居所】　東京都渋谷区神宮前４－２－１９
【氏名】　辻井　重男
【発明者】
【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内
【氏名】　村上　恭通
【発明者】
【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号
【氏名】　笠原　正雄
【特許出願人】
【識別番号】　000006297
【氏名又は名称】　村田機械株式会社
【代表者】　村田　純一
【特許出願人】
【住所又は居所】　東京都渋谷区神宮前４－２－１９
【氏名又は名称】　辻井　重男
【特許出願人】
【識別番号】　597008636
【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　秘密鍵生成方法，暗号化方法及び暗号通信方法

【特許請求の範囲】

【請求項１】　センタから各エンティティへ送付すべき各エンティティ固有の秘密鍵を生成する方法において、前記各エンティティの特定情報を分割した分割特定情報を利用して、前記各エンティティ固有の秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項２】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、エンティティが前記センタから送付された該エンティティ固有の秘密鍵を利用して平文を暗号文に暗号化する暗号化方法において、前記各エンティティの特定情報を分割した分割特定情報を利用して、前記各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化することを特徴とする暗号化方法。

【請求項３】　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにしたことを特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、エンティティ固有の秘密鍵を生成する秘密鍵生成方法、情報の内容

が当事者以外にはわからないように情報を暗号化する暗号化方法、及び、暗号文にて通信を行う暗号通信方法に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。このような共通鍵暗号方式の従来例は、次のような３種の方法に分類できる。

【０００５】

①　第１の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法。

② 第２の方法

暗号通信の都度、予備通信により鍵を共有し合う方法（Diffie-Hellmanによる鍵共有方式，公開鍵方式による鍵配送方式など）。

③ 第３の方法

各ユーザ（エンティティ）の氏名，住所などの個人を特定する公開された特定情報（ＩＤ（Identity）情報）を利用して、予備通信を行うことなく、送信側のエンティティ，受信側のエンティティが独立に同一の共通鍵を生成する方法（ＫＰＳ（Key Predistribution System），ＩＤ－ＮＩＫＳ（ID-based Non-Interactive Key Sharing Schemes）など）。

【０００６】

【発明が解決しようとする課題】

このような従来の３種の方法には、以下に述べるような問題がある。第１の方法では、すべての共通鍵を保管しておくようにするので、不特定多数のユーザがエンティティとなって暗号通信を行うネットワーク社会には適さない。また、第２の方法は、鍵共有のための予備通信が必要である点が問題である。

【０００７】

第３の方法は、予備通信が不要であり、公開された相手のＩＤ情報とセンタから予め配布されている固有の秘密パラメータとを用いて、任意の相手との共通鍵を生成できるので、便利な方法である。しかしながら、次のような２つの問題点がある。一つは、センタがBig Brother となる（すべてのエンティティの秘密を握っており、Key Escrow System になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【０００８】

この結託問題の難しさは、ＩＤ情報に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。第３の方法では、センタの公

開パラメータと個人の公開ＩＤ情報とこの２種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【０００９】

本発明は斯かる事情に鑑みてなされたものであり、特定情報（ＩＤ情報）をいくつかに分割し、複数の各センタからその分割した特定情報に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる秘密鍵生成方法，暗号化方法及び暗号通信方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】

請求項１に係る秘密鍵生成方法は、センタから各エンティティへ送付すべき各エンティティ固有の秘密鍵を生成する方法において、前記各エンティティの特定情報を分割した分割特定情報を利用して、前記各エンティティ固有の秘密鍵を生成することを特徴とする。

【００１１】

請求項２に係る暗号化方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、エンティティが前記センタから送付された該エンティティ固有の秘密鍵を利用して平文を暗号文に暗号化する暗号化方法において、前記各エンティティの特定情報を分割した分割特定情報を利用して、前記各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化することを特徴とする。

【００１２】

請求項３に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方

のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにしたことを特徴とする。

【００１３】

結託問題を解決することを目的として提案されてきたエンティティの特定情報に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、本発明では、エンティティの特定情報をいくつかに分割し、分割した各特定情報についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【００１４】

本発明では、複数のセンタが設けられ、各センタはあるエンティティの分割した１つの特定情報に対応する秘密鍵を生成する。よって、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。また、数学的構造を最小限に抑えているので、結託問題の回避を実現しやすく、また、暗号系の実現も容易となる。更に、各エンティティが共通鍵を生成するための自身固有の秘密鍵をセンタから送付されて予めテーブル形式で保持しているので、共通鍵生成に要する時間を大幅に短くできる。

【００１５】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｋ個）のセンタ１が設定されており、これらのセンタ１として

は、例えば社会の公的機関を該当できる。このように複数のセンタ１を設けた点が従来の第３の方法とは異なる。

【００１６】

これらの各センタ１と、この暗号系システムを利用するユーザとしての複数の各エンティティａ，ｂ，…，ｚとは、秘密通信路2_{a1}，…，2_{aK}、2_{b1}，…，2_{bK}、・・・、2_{z1}，…，2_{zK}により接続されており、これらの秘密通信路を介して各センタ１から秘密の鍵情報が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００１７】

〔第１実施の形態〕

まず、本発明の基本方式である第１実施の形態について説明する。

【００１８】

（センタ１での準備処理）

センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　Ｐ　大きな素数

Ｌ　ＩＤベクトルのサイズ（Ｌ＝ＫＭ）

Ｋ　ＩＤベクトルの分割ブロック数

Ｍ　分割したＩＤベクトルのサイズ

秘密鍵　g　ＧＦ（Ｐ）の原始元

H_j　乱数からなる$2^M \times 2^M$の対称行列

（ｊ＝１，２，・・・，Ｋ）

α_{ij}　エンティティｉの個人秘密乱数

（但し、$\alpha_{i1}\alpha_{i2}\cdots\alpha_{iK} \equiv 1 \pmod{P-1}$）

【００１９】

各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、図２に示すようにそのＩＤベクトルをブロックサイズＭ毎にＫ個のブロックに分割する。例えば、エンティティｉのＩＤベクトル（ベクトル

I_i）を式（1）のように分割する。分割特定情報である各ベクトルI_{ij}（j＝1，2，・・・，K）をＩＤ分割ベクトルと呼ぶ。

【００２０】

【数１】

$$\overrightarrow{I_i} = [\overrightarrow{I_{i1}} | \overrightarrow{I_{i2}} | \cdots | \overrightarrow{I_{iK}}] \quad \cdots(1)$$

【００２１】

（エンティティの登録処理）

エンティティｉに登録を依頼された各センタ１は、準備した鍵とエンティティｉのＫ個のＩＤ分割ベクトルについて、それぞれに対応するＫ個の秘密鍵ベクトルs_{ij}（j＝1，2，・・・，K）を以下の式（2-1），（2-2），・・・，（2-K）に従って求め、求めたベクトルs_{ij}を秘密裏に送って、登録を完了する。

【００２２】

【数２】

$$\overrightarrow{s_{i1}} \equiv g^{\alpha_{i1} H_1[\overrightarrow{I_{i1}}]} \pmod{P} \quad \cdots(2-1)$$

$$\overrightarrow{s_{i2}} \equiv \alpha_{i2} H_2[\overrightarrow{I_{i2}}] \pmod{P-1} \quad \cdots(2-2)$$

$$\vdots$$

$$\overrightarrow{s_{iK}} \equiv \alpha_{iK} H_K[\overrightarrow{I_{iK}}] \pmod{P-1} \quad \cdots(2-K)$$

【００２３】

但し、ｇをスカラー、Ａ，Ｂを行列とした場合、$B = g^A$ はＡの各（μ，ν）成分についてｇのべき乗を行うことを表す。即ち、式（３）のようになる。また、H_j［ベクトルI_{ij}］は対称行列H_jからベクトルI_{ij}に対応した行を１行抜き出したものを表し、［・］の操作を参照と定義する。

【００２４】

【数３】

$$B_{\mu\nu} = g^{A\mu\nu} \qquad \cdots(3)$$

【００２５】

（エンティティ間の共通鍵の生成処理）

エンティティｉは、自身の秘密鍵ベクトルs_{i1}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{m1}に対応する成分のベクトルs_{i1}［ベクトルI_{m1}］を選び出し、また、ｊ＝２，・・・，Ｋの各ブロックについて秘密鍵ベクトルs_{ij}の中から、ベクトルI_{mj}に対応する成分のベクトルs_{ij}［ベクトルI_{mj}］を各ブロック毎に選び出す。そして、Ｐを法とし、ベクトルs_{i1}［ベクトルI_{m1}］を底として残りのすべてのベクトルs_{ij}［ベクトルI_{mj}］（ｊ＝２，・・・，Ｋ）を順次べき乗することにより、共通鍵K_{im}を求める。このK_{im}を求める演算式は具体的に式（４）となり、このK_{im}はエンティティｍ側から求めた共通鍵K_{mi}と一致する。

【００２６】

【数４】

$$\begin{aligned} K_{im} &\equiv \overrightarrow{s_{i1}}[\overrightarrow{I_{m1}}]^{\overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]\cdots\overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]} \\ &\equiv g^{\alpha_{i1}\cdots\alpha_{iK}H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]\cdots H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]} \\ &\equiv g^{H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]\cdots H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]} \pmod P \end{aligned} \qquad \cdots(4)$$

【００２７】

次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図３は、２人のエンティティａ，ｂ間における情報の通信状態を示す模

式図である。図２の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ伝送し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００２８】

ｊ（ｊ＝１，２，・・・，Ｋ）番目のセンタ１には、各エンティティａ，ｂ固有のベクトルs_{aj}，s_{bj}（秘密鍵）を前記式（2-j)に従って求める秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵ベクトルs_{aj}，s_{bj}がエンティティａ，ｂへ送付される。

【００２９】

エンティティａ側には、Ｋ個の各センタ１から送られる固有の秘密鍵ベクトルs_{a1}，…，s_{aj}，…，s_{aK}をテーブル形式で格納しているメモリ１０と、これらの秘密鍵ベクトルの中からエンティティｂに対応する成分であるベクトルs_{a1}［ベクトルI_{b1}］，…，ベクトルs_{aj}［ベクトルI_{bj}］，…，ベクトルs_{aK}［ベクトルI_{bK}］を選び出す成分選出器１１と、選び出されたこれらの成分を使用してエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成器１２と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００３０】

また、エンティティｂ側には、各センタ１から送られる固有の秘密鍵ベクトルs_{b1}，…，s_{bj}，…，s_{bK}をテーブル形式で格納しているメモリ２０と、これらの秘密ベクトルの中からエンティティａに対応する成分であるベクトルs_{b1}［ベクトルI_{a1}］，…，ベクトルs_{bj}［ベクトルI_{aj}］，…，ベクトルs_{bK}［ベクトルI_{aK}］を選び出す成分選出器２１と、選び出されたこれらの成分を使用してエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成器２２と、共通鍵K_{ba}を用いて通信路30から入力した暗号文Ｃを平文（メッセージ）Ｍに復号して出力する復号器２３とが備えられている。

【００３１】

エンティティａからエンティティｂへ情報を伝送しようとする場合、まず、各

センタ１で式（2-1），（2-2），…，（2-K)に従って求められて、予めメモリ１０に格納されている秘密鍵ベクトルs_{a1}，s_{a2}，…，s_{aK}が成分選出器１１へ読み出される。そして、成分選出器11にて、エンティティｂに対応する成分であるベクトルs_{a1}［ベクトルI_{b1}］，ベクトルs_{a2}［ベクトルI_{b2}］，…，ベクトルs_{aK}［ベクトルI_{bK}］が選び出されて共通鍵生成器１２へ送られる。共通鍵生成器１２にて、これらの成分を使用して式（４）に従って共通鍵K_{ab}が求められ、暗号化器１３へ送られる。暗号化器１３において、この共通鍵K_{ab}を用いて平文（メッセージ）Ｍが暗号文Ｃに暗号化され、暗号文Ｃが通信路３０を介して伝送される。

【００３２】

通信路３０を伝送された暗号文Ｃはエンティティｂの復号器２３へ入力される。各センタ１で式（2-1），（2-2），…，（2-K)に従って求められて、予めメモリ２０に格納されている秘密鍵ベクトルs_{b1}，s_{b2}，…，s_{bK}が成分選出器２１へ読み出される。そして、成分選出器２１にて、エンティティａに対応する成分であるベクトルs_{b1}［ベクトルI_{a1}］，ベクトルs_{b2}［ベクトルI_{a2}］，…，ベクトルs_{bK}［ベクトルI_{baK}］が選び出されて共通鍵生成器２２へ送られる。共通鍵生成器２２にて、これらの成分を使用して式（４）に従って共通鍵K_{ba}が求められ、復号器２３へ送られる。復号器２３において、この共通鍵K_{ba}を用いて暗号文Ｃが平文（メッセージ）Ｍに復号される。

【００３３】

本発明の方式では、各エンティティ固有の秘密鍵ベクトルが予めエンティティ側のメモリに格納されているので、共通鍵生成に要する時間が短くて済む。

【００３４】

次に、本発明の方式における安全性について説明する。

安全なＩＤ－ＮＩＫＳの必要条件として、秘密鍵生成関数及び鍵共有関数が多項式時間で分離できないことが知られている。以下に、本発明の方式がこの必要条件を満たすことを示す。

【００３５】

（秘密鍵生成関数）

本発明の方式は、式（５），（６）に示すＫ個の秘密鍵生成関数を有する。

【００３６】

【数５】

$$f_1(\vec{x}) = g^{\alpha_{i1} H_1[\vec{x}]} \quad (j=1) \quad \cdots(5)$$

$$f_j(\vec{x}) = \alpha_{ij} H_j[\vec{x}] \quad (j=2,\ldots,K) \quad \cdots(6)$$

【００３７】

Ｈを任意の対称行列した場合、式（７），（８）に示すように、参照関数［・］は明らかに分離不可能である。

【００３８】

【数６】

$$H[\vec{x}+\vec{y}] \neq H[\vec{x}]+H[\vec{y}] \quad \cdots(7)$$

$$H[\vec{x}+\vec{y}] \neq H[\vec{x}] \cdot H[\vec{y}] \quad \cdots(8)$$

【００３９】

従って、前記式（５），（６）で表されるＫ個の秘密鍵生成関数は、式（９）に示すように、分離不可能である。

【００４０】

【数７】

$$f_j(\vec{x}+\vec{y}) \neq f_j(\vec{x}) \circ f_j(\vec{y}) \quad (j=1,2,\ldots,K) \quad \cdots(9)$$

【００４１】

（鍵共有関数）

本発明の方式における鍵共有関数を、式（10）に示す。

【００４２】

【数８】

$$F(\vec{x},\vec{y})=g^{H_1[\vec{x_1}][\vec{y_1}]\cdots H_K[\vec{x_K}][\vec{y_K}]} \quad \cdots(10)$$

【００４３】

秘密鍵生成関数の場合と同様に、式（10）で表される鍵共有関数は、式（11）に示すように、分離不可能である。

【００４４】

【数９】

$$F(\vec{a},\vec{x}+\vec{y})\neq F(\vec{a},\vec{x})\circ F(\vec{a},\vec{y}) \quad \cdots(11)$$

【００４５】

従来より、不特定多数のエンティティの結託によって暗号システム全体を破る攻撃（以下、非買収結託という）が議論されている。一方、ある特定の個人のみを攻撃する場合には、攻撃に必要なエンティティのみを買収して、より少ない数の結託者にて行う攻撃（以下、買収結託という）も有効である。以下、これらの非買収結託，買収結託に対する本発明の方式の安全性について考察する。

【００４６】

（非買収結託に対する安全性）

任意のエンティティのＩＤベクトルを結託者のＩＤベクトルの線形結合で表現すること（結合攻撃）ができ、しかも、秘密鍵生成関数または鍵共有関数が多項式時間で分離可能である場合には、他のエンティティの秘密鍵を結託者の秘密鍵から偽造すること（分離攻撃）が可能である。このような攻撃を線形攻撃という。

【００４７】

本発明の方式でも、一次独立なＬ人の結託者のＩＤベクトルを使用することにより、任意のエンティティのＩＤベクトルを線形結合として表現することができる。つまり、Ｌ人以上のエンティティによる結合攻撃は成立する。しかしながら、前述したように秘密鍵生成関数及び鍵共有関数が分離不可能な関数であるので、万一任意のエンティティに対して結合攻撃が成立した場合においても、そのエンティティの秘密鍵及び共通鍵を分離攻撃によって偽造することはできない。よって、本発明の方式には線形攻撃が通用しない。従って、非買収結託に対して本発明の方式は、Ｌよりはるかに高い結託閾値（結合攻撃に必要な最小の結託者数）を有する。

【００４８】

（買収結託に対する安全性）

本発明の方式に対して、特定のエンティティを攻撃する場合には、攻撃に必要なすべてのエンティティを買収し、買収したエンティティの秘密鍵のすべてを用いることによる以下のような乱数置換攻撃が考えられる。

【００４９】

エンティティのＩＤを分かりやすいように氏名の漢字４文字（Ｌ＝４×16＝64ビット）とし、漢字１文字を１ブロックとした例で説明する。即ち、Ｋ＝４，Ｍ＝16と設定する。

【００５０】

エンティティＺ，Ａ，Ｂ，Ｃ，ＤのＩＤを以下のように設定し、エンティティＡ，Ｂ，Ｃ，Ｄを買収してエンティティＺを攻撃する場合について考える。

【００５１】

【数１０】

$$\overrightarrow{I_Z} = [辻 | 井 | 重 | 男]$$
$$\overrightarrow{I_A} = [辻 | 本 | 恵 | 子]$$
$$\overrightarrow{I_B} = [中 | 井 | 邦 | 夫]$$
$$\overrightarrow{I_C} = [山 | 田 | 重 | 人]$$
$$\overrightarrow{I_D} = [佐 | 藤 | 和 | 男]$$

【００５２】

エンティティＺの秘密鍵は以下のようになる。

【００５３】

【数１１】

$$\overrightarrow{s_{Z1}} \equiv g^{\alpha_{Z1}} H_1[辻] \quad (\mathrm{mod}\ P)$$
$$\overrightarrow{s_{Z2}} \equiv \alpha_{Z2} H_2[井] \quad (\mathrm{mod}\ P-1)$$
$$\overrightarrow{s_{Z3}} \equiv \alpha_{Z3} H_3[重] \quad (\mathrm{mod}\ P-1)$$
$$\overrightarrow{s_{Z4}} \equiv \alpha_{Z4} H_4[男] \quad (\mathrm{mod}\ P-1)$$

【００５４】

結託者は以下のような計算を行って、エンティティＺの秘密鍵を偽造する。

【００５５】

【数１２】

$$\overrightarrow{s_{Z1}}' \equiv \overrightarrow{s_{A1}} \equiv g^{\alpha_{A1}H_1[辻]} \quad (\mathrm{mod}\ P)$$

$$\overrightarrow{s_{Z2}}' \equiv \frac{\overrightarrow{s_{A2}}[井]}{\overrightarrow{s_{B2}}[本]} \cdot \overrightarrow{s_{B2}} \equiv \frac{\alpha_{A2}H_2[本][井]}{\alpha_{B2}H_2[井][本]} \cdot \alpha_{B2}H_2[井]$$

$$\equiv \alpha_{A2}H_2[井] \quad (\mathrm{mod}\ P-1)$$

$$\overrightarrow{s_{Z3}}' \equiv \frac{\overrightarrow{s_{A3}}[重]}{\overrightarrow{s_{C3}}[恵]} \cdot \overrightarrow{s_{C3}} \equiv \frac{\alpha_{A3}H_3[恵][重]}{\alpha_{C3}H_3[重][恵]} \cdot \alpha_{C3}H_3[重]$$

$$\equiv \alpha_{A3}H_3[重] \quad (\mathrm{mod}\ P-1)$$

$$\overrightarrow{s_{Z4}}' \equiv \frac{\overrightarrow{s_{A4}}[男]}{\overrightarrow{s_{D4}}[子]} \cdot \overrightarrow{s_{D4}} \equiv \frac{\alpha_{A4}H_4[子][男]}{\alpha_{D4}H_4[男][子]} \cdot \alpha_{D4}H_4[男]$$

$$\equiv \alpha_{A4}H_4[男] \quad (\mathrm{mod}\ P-1)$$

【００５６】

偽造したベクトルs_{Z1}'～ベクトルs_{Z4}'はそれぞれベクトルs_{Z1}～ベクトルs_{Z4}と同等の働きをすることが分かる。このように、本発明の方式に対して、攻撃に必用なエンティティを買収することが可能である状況では、確かに結託攻撃が成立する。

【００５７】

しかしながら、このような買収結託攻撃が成立するためには、攻撃目標のエンティティのＫ個のすべてのＩＤ分割ベクトルに対し、全く同一のＩＤ分割ベクトルを有する結託者の秘密鍵を入手する必要がある。ある特定のブロックについて、全く同一のＩＤ分割ベクトルを有するエンティティは2^M人に１人であり、この特別なエンティティをＫブロックすべて買収することは、Ｍ＝10，Ｋ＝100 程度としても、現実的には容易でない。従って、買収結託に対しても本発明の方式は安全であると言える。なお、パラメータＭ，Ｋは、暗号システムの規模及び／または要求される安全性の程度に応じて適切に設定することができる。

【００５８】

図４は、本発明の記録媒体の実施例の構成を示す図である。ここに例示するプログラムは、各センタから送られてくる秘密鍵ベクトルs_{ij}の中からエンティティｍに対応する成分を選び出す処理と、これらの選び出した成分を使用して式（４）に従って共通鍵K_{im}を求める処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各エンティティ側に設けられている。

【００５９】

図４において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【００６０】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【００６１】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュータ４０を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【００６２】

ところで、買収結託による乱数置換攻撃を回避するためには、分割ブロックが

独立して攻撃されないような工夫を施せば良い。即ち、全ブロックすべての計算を完了して初めて乱数項が消去されるようにすれば良い。このような観点に基づいて第１実施の形態を改良した２つの実施の形態について、以下に説明する。

【００６３】

〔第２実施の形態〕

乱数消去方法を組み合わせることにより、乱数置換攻撃に対して強化した本発明の他の例（第２実施の形態）を説明する。

【００６４】

（センタ１での準備処理）

第１実施の形態と同様に、センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　Ｐ　大きな素数

Ｌ　ＩＤベクトルのサイズ（Ｌ＝ＫＭ）

Ｋ　ＩＤベクトルの分割ブロック数

Ｍ　分割したＩＤベクトルのサイズ

秘密鍵　ｇ　ＧＦ（Ｐ）の原始元

H_j　乱数からなる$2^M \times 2^M$の対称行列

（ｊ＝１，２，・・・，Ｋ）

α_i　エンティティｉの個人秘密乱数

（但し、$\alpha_{i1}\alpha_{i2}\cdots\alpha_{iK} \equiv 1 \pmod{P-1}$）

【００６５】

なお、ＲＳＡ暗号の安全性を用いるため、Ｐ－１を素因数分解することが困難となるようにＰを設定する。このようにするためには、Ｐ＝２ｐｑ＋１（ｐ，ｑ：素数）となる素数を使用すれば良い。

【００６６】

また、第１実施の形態と同様に、各エンティティのＩＤベクトルを、ブロックサイズＭのＫ個のブロック（ＩＤ分割ベクトル）に分割する（図２，式（１）参照）。

【００６７】

更に、式（12）に示すようにＩＤからＫ－１次元の第２ＩＤベクトルv_iを生成するハッシュ関数ｈ（・）をセンタ１は公開する。但し、このハッシュ関数で生成された第２ＩＤベクトルv_iの各成分は正の整数をとり、式（13）に示すように、それらの和は比較的小さな定数ｅになるとする。

【００６８】

【数１３】

$$\overrightarrow{v_i} = (v_{i2}, v_{i3}, \cdots, v_{iK}) = h(ID_i) \quad \cdots(12)$$

$$\sum_{j=2}^{K} v_{ij} = e \quad \cdots(13)$$

【００６９】

（エンティティの登録処理）

エンティティｉに登録を依頼された各センタ１は、準備した鍵とエンティティｉのＫ個のＩＤ分割ベクトルについて、それぞれに対応するＫ個の秘密鍵ベクトルs_{ij}（ｊ＝１，２，・・・，Ｋ）を以下の式（14-1），（14-2），・・・，（14-Ｋ）に従って求め、求めたベクトルs_{ij}を秘密裏に送って、登録を完了する。

【００７０】

【数１４】

$$\overrightarrow{s_{i1}} \equiv g^{\alpha_i^{-e}} H_1[\overrightarrow{I_{i1}}] \pmod{P} \quad \cdots(14\text{-}1)$$

$$\overrightarrow{s_{i2}} \equiv \alpha_i H_2[\overrightarrow{I_{i2}}]^{v_{i2}} \pmod{P-1} \quad \cdots(14\text{-}2)$$

$$\vdots$$

$$\overrightarrow{s_{iK}} \equiv \alpha_i H_K[\overrightarrow{I_{iK}}]^{v_{iK}} \pmod{P-1} \quad \cdots(14\text{-}K)$$

【００７１】

（エンティティ間の共通鍵の生成処理）

エンティティｉは、公開されているハッシュ関数ｈ（・）を用いて、相手のエ

ンティティｍの第２ＩＤベクトルのベクトルv_mを式（15）に従って求める。

【００７２】

【数１５】

$$\overrightarrow{v_m}=(v_{m2}, v_{m3}, \cdots, v_{mK})=h(ID_m) \quad \cdots(15)$$

【００７３】

エンティティｉは、自分の秘密鍵ベクトルs_{i1}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{m1}に対応する成分のベクトルs_{i1}［ベクトルI_{m1}］を選び出し、また、ｊ＝２，・・・，Ｋの各ブロックについて秘密鍵ベクトルs_{ij}の中から、ベクトルI_{mj}に対応する成分のベクトルs_{ij}［ベクトルI_{mj}］を各ブロック毎に選び出す。そして、Ｐを法とし、ベクトルs_{i1}［ベクトルI_{m1}］を底として残りのすべてのベクトルs_{ij}［ベクトルI_{mj}］（ｊ＝２，・・・，Ｋ）を順次v_{mj}回ずつ繰り返しべき乗することにより、共通鍵K_{im}を求める。このK_{im}を求める演算式は具体的に式（16）となり、このK_{im}はエンティティｍ側から求めた共通鍵K_{mi}と一致する。

【００７４】

【数１６】

$$K_{im} \equiv \overrightarrow{s_{i1}}[\overrightarrow{I_{m1}}]^{\overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]^{v_{m2}} \cdots \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]^{v_{mK}}}$$

$$\equiv g^{\alpha_i^{-e}\,\alpha_i^{e}\cdot H_{1[i1][m1]}\cdot H_{2[i2][m2]}^{v_{m2}} \cdots H_{K[iK][mK]}^{v_{mK}}}$$

$$\equiv g^{H_{1[i1][m1]}\cdot H_{2[i2][m2]}^{v_{i2}v_{m2}} \cdots H_{K[iK][mK]}^{v_{iK}v_{mK}}} \pmod P$$

$$\cdots(16)$$

但し，第二式以降，$[\overrightarrow{I_{ij}}]$を$[I_{ij}]$と略記

【００７５】

（乱数置換攻撃に対する安全性）

前記のエンティティＡ，Ｂの実例において、一般に$v_{A2} \neq v_{B2}$となるので、以下の式（17）に示すように、乱数置換攻撃は成立しない。

【００７６】

【数１７】

$$\overrightarrow{s_{Z2}}' \equiv \frac{\overrightarrow{s_{A2}}[井]}{\overrightarrow{s_{B2}}[本]} \cdot \overrightarrow{s_{B2}}$$

$$\equiv \frac{\alpha_A H_2[本][井]^{v_{A2}}}{\alpha_B H_2[井][本]^{v_{B2}}} \cdot \alpha_B H_2[井]$$

$$\neq \alpha_A H_2[井] \quad (\mathrm{mod}\ P-1) \qquad \cdots(17)$$

【００７７】

〔第３実施の形態〕

定数項を追加することにより、個人乱数消去のプロセスを複雑にした本発明の他の例（第３実施の形態）を説明する。

【００７８】

（センタ１での準備処理）

第１実施の形態と同様に、センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　Ｎ　　Ｎ＝ＰＱ（Ｐ，Ｑ：大きな素数）

Ｌ　　ＩＤベクトルのサイズ（Ｌ＝ＫＭ）

Ｋ　　ＩＤベクトルの分割ブロック数

Ｍ　　分割したＩＤベクトルのサイズ

秘密鍵　ｇ　　Ｎを法とする最大生成元

H_j　乱数からなる$2^M \times 2^M$の対称行列

（ｊ＝１，２，・・・，Ｋ）

α_{ij}　エンティティｉの個人秘密乱数

（但し、$\alpha_{i1}\alpha_i\ \alpha_{iK}\equiv 1 \pmod{\lambda(N)}$

$\lambda(\cdot)$はカーマイケル関数）

【００７９】

また、第１実施の形態と同様に、各エンティティのＩＤベクトルを、ブロックサイズＭのＫ個のブロック（ＩＤ分割ベクトル）に分割する（図２，式（１）参照）。

【００８０】

（エンティティの登録処理）

エンティティｉに登録を依頼された各センタ１は、準備した鍵とエンティティｉのＫ個のＩＤ分割ベクトルについて、それぞれに対応するＫ個の秘密鍵ベクトルs_{ij}（ｊ＝１，２，・・・，Ｋ－１，Ｋ）を以下の式（18-1），（18-2），・・・，（18-K-1），（18-K）に従って求める。

【００８１】

【数１８】

$$\overrightarrow{s_{i1}} \equiv g^{\alpha_{i1}H_1[\overrightarrow{I_{i1}}]} \pmod{N} \quad \cdots(18\text{-}1)$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}]+\beta_{i2} \quad \cdots(18\text{-}2)$$

$$\vdots$$

$$\overrightarrow{s_{i,K-1}} = \alpha_i H_{K-1}[\overrightarrow{I_{i,K-1}}]+\beta_{i,K-1} \quad \cdots(18\text{-}K\text{-}1)$$

$$\overrightarrow{s_{iK}} = \alpha_{iK} H_K[\overrightarrow{I_{iK}}] \quad \cdots(18\text{-}K)$$

【００８２】

第３実施の形態は、第１実施の形態において、$\alpha_{i2}=\cdots\alpha_{i,K-1}=\alpha_i$とし、$\alpha_{i1}\alpha_i\ \alpha_{iK}\equiv 1 \pmod{\lambda(N)}$としたものに、更にＫ－２個の個人乱数$\beta_{i2}$，・・・，$\beta_{i,K-1}$を追加したものである。センタ１は、式（19）に従って

、ベクトルt_iを求める。但し、$\beta_i = \beta_{i2} + \cdots + \beta_{i,K-1}$とする。求めたベクトル$s_{ij}$及びベクトル$t_i$を秘密裏に送って、登録を完了する。

【００８３】

【数１９】

$$\overrightarrow{t_i} \equiv g^{-\alpha_{i1} H_1[\overrightarrow{I_{i1}}]\beta_i} \pmod N \quad \cdots(19)$$

【００８４】

（エンティティ間の共通鍵の生成処理）

エンティティｉは、まず、ｊ＝２，・・・，Ｋ－１の各ブロックについて秘密鍵ベクトルs_{ij}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{mj}に対応する列ベクトルs_{ij}［ベクトルI_{mj}］を各ブロック毎に選び出し、それらのすべての和S_{im}を、式（20）のように求める。

【００８５】

【数２０】

$$S_{im} = \sum_{j=2}^{K-1} \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$

$$= \alpha_i \sum_{j=2}^{K-1} H_j[\overrightarrow{I_{ij}}][\overrightarrow{I_{mj}}] + \beta_i \quad \cdots(20)$$

【００８６】

更に、エンティティｉは、自身の最初のブロックの秘密鍵ベクトルs_{i1}及び最後のブロックの秘密鍵ベクトルs_{iK}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{mj}に対応する列を選び出し、S_{im}とベクトルt_iとを用いて、以下の式（21）のような計算を行って、共通鍵K_{im}を求める。このK_{im}はエンティティｍ側から求めた共通鍵K_{mi}と一致する。

【００８７】

【数２１】

$$K_{im} \equiv \left(\overrightarrow{t_i[I_{m1}]} \cdot \overrightarrow{s_{i1}[I_{m1}]}^{S_{im}} \right)^{\overrightarrow{s_{iK}[I_{mK}]}}$$

$$\equiv g^{\alpha_{i1}\alpha_{i1}\alpha_{iK}H_1[i1][m1]\left(\sum_{J=2}^{K-1} H_J[ij][mj]\right)H_K[iK][mK]}$$

$$\equiv g^{H_1[i1][m1]\left(\sum_{J=2}^{K-1} H_J[ij][mj]\right)H_K[iK][mK]}$$

$$(\mathrm{mod}\ N) \quad \cdots (21)$$

但し，第二式以降，$[\overrightarrow{I_{ij}}]$を$[ij]$と略記

【００８８】

（安全性の考察）

この方式では、式（22）のように設定すれば、$K_{im}=x_{im2}\ x_{im3}\ \cdots\ x_{im,K-1}$と表記でき、$x_{im2}$，$x_{im3}$，・・・，$x_{im,K-1}$を変数とする方程式を多数集めた場合には、原理的には鍵を偽造することができる。

【００８９】

【数２２】

$$x_{i\,m_2} = g^{H_{1[i1][m1]}\,H_{2[i2][m2]}\,H_{K[iK][mK]}}$$

$$x_{i\,m_3} = g^{H_{1[i1][m1]}\,H_{3[i3][m3]}\,H_{K[iK][mK]}}$$

$$\vdots$$

$$x_{i\,m,K-1} = g^{H_{1[i1][m1]}\,H_{K-1[i,K-1][m,K-1]}\,H_{K[iK][mK]}}$$

・・・(22)

【００９０】

しかしながら、本発明の方式では、数学的構造を最小限に抑えており、これらの変数に分離可能という構造がないので、これらのすべての変数を独立変数として攻撃しなければならず、非常に莫大な数の結託者を必要とする。最終ブロックは乱数置換攻撃で消去するようにしても、式（22）に示す項を独立変数として攻撃しなければならないので、例えばＭ＝10の場合、2^{20}もの特定の方程式を集めて攻撃する必要があり、安全性が向上している。

【００９１】

なお、第３実施の形態では、法として素因数分解が困難な合成数Ｎを用いる場合について説明したが、Ｎ＝Ｐの場合も同様に行えることは勿論である。

【００９２】

【発明の効果】

以上詳述したように、本発明では、複数のセンタが設けられ、各センタはエンティティの分割した１つのＩＤ情報に対応する鍵を生成するようにしたので、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。また、数学的構造を最小限に抑えているので、結託問題の回避を実現しやすく、また、暗号系の実現も容易である。更に、各エンティティが固有の秘密鍵を予め保持しているので、共通鍵生成に要する時間を大幅に短くできる。

【００９３】

前述した従来の第３の方法によるＩＤ－ＮＩＫＳでは、一般的に、Ｌ×Ｌの対称行列をセンタ秘密として、その情報の一部をＬ個の成分からなるベクトルとしてエンティティに配布しており、実現は非常に容易であるが結託閾値はＬ程度に過ぎない。これに対して、本発明の方式では、このＬよりはるかに高い結託閾値を持つことができる。

【００９４】

従来の方式でも、$2^M \times 2^M$ のセンタ秘密行列を用いることにより、本発明と同程度の結託閾値を有するＩＤ－ＮＩＫＳを構成することは可能である。しかしながら、そのように構成されたＩＤ－ＮＩＫＳでは、鍵共有に 2^M 回の積演算またはべき乗演算が必要であって実用的ではなく、ほとんどの方式が分離可能であって一部の結託者の線形結合で表されたエンティティの秘密鍵が偽造されてしまうという問題がある。これに対して、本発明の方式では、保持する秘密鍵の数は多くなるが、多くともＫ－１回のべき乗演算にて共通鍵を共有することができ、鍵生成が非常に高速で行え、しかも、例え一部のエンティティが結託者の線形結合で表されたとしても、それらのエンティティの秘密鍵が偽造されるのを防ぐことができる。

【００９５】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティテ

ィの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにしており、各エンティティの分割特定情報に前記各エンティティ固有の乱数を加えて、前記各エンティティ固有の秘密鍵を生成する暗号通信方法。

（２）　第（１）項記載の暗号通信方法であって、前記各センタにおける秘密鍵を生成する演算式は以下である暗号通信方法。

【００９６】

【数２３】

$$\overrightarrow{s_{i1}} \equiv g^{\alpha_{i1} H_1[\overrightarrow{I_{i1}}]} \quad (\mathrm{mod}\ P)$$

$$\overrightarrow{s_{i2}} \equiv \alpha_{i2} H_2[\overrightarrow{I_{i2}}] \quad (\mathrm{mod}\ P-1)$$

$$\vdots$$

$$\overrightarrow{s_{iK}} \equiv \alpha_{iK} H_K[\overrightarrow{I_{iK}}] \quad (\mathrm{mod}\ P-1)$$

【００９７】

但し、

ベクトルs_{ij}：エンティティｉのｊ番目の分割特定情報に対応する秘密鍵（ｊ＝１，２，・・・，Ｋ）

［ベクトルI_{ij}］：エンティティｉのｊ番目の分割特定情報

Ｐ：素数

Ｋ：エンティティｉの特定情報の分割数

ｇ：ＧＦ（Ｐ）の原始元

H_j：乱数からなる$2^M \times 2^M$の対称行列

Ｍ：エンティティｉの特定情報の分割サイズ

α_{ij}：エンティティｉの個人秘密乱数

（但し、$\alpha_{i1} \cdots \alpha_{iK} \equiv 1 \pmod{P-1}$）

（３）　第（２）項記載の暗号通信方法であって、各エンティティにおける共通

鍵を生成する演算式は以下である暗号通信方法。

【００９８】

【数２４】

$$K_{im} \equiv \overrightarrow{s_{i1}[I_{m1}]}^{\overrightarrow{s_{i2}[I_{m2}]}\cdots\overrightarrow{s_{iK}[I_{mK}]}}$$

$$\equiv g^{\alpha_{i1}\cdots\alpha_{iK}H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]\cdots H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]}$$

$$\equiv g^{H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]\cdots H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]} \pmod P$$

【００９９】

但し、

K_{im}：一方のエンティティｉが他方のエンティティｍに対して生成する共通鍵

ベクトルs_{ij}［ベクトルI_{ij}］：エンティティｉの秘密鍵ベクトルs_{ij}に含まれ、エンティティｍの分割特定情報に対応する成分

（４）　暗号通信システムのエンティティに設けられており、平文から暗号文への暗号化処理及び暗号文から平文への復号処理の用いる共通鍵を生成する共通鍵生成装置において、前記エンティティの特定情報を分割した分割特定情報毎に作成された前記エンティティ固有の秘密鍵を格納する格納手段と、格納されている秘密鍵の中から、通信相手のエンティティの分割特定情報に対応する成分を選び出す選出手段と、選び出した成分を使用して前記共通鍵を生成する手段とを備える共通鍵生成装置。

（５）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行う暗号通信システムにおいて、各エンティティの特定情報を分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成して各エンティティへ送付

する複数のセンタと、該センタから送付された自身の秘密鍵に含まれている、通信対象のエンティティの分割特定情報に対応する成分を使用して、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システム。

（６）　暗号通信システムにおける平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵をエンティティ側で生成するためのプログラムを記録してあるコンピュータでの読み取り可能な記録媒体において、前記エンティティの特定情報を分割した分割特定情報毎に作成された前記エンティティ固有の秘密鍵の中から、通信相手のエンティティの分割特定情報に対応する成分を選び出すことを前記コンピュータにさせるプログラムコード手段と、選び出した成分を使用して前記共通鍵を生成することを前記コンピュータにさせるプログラムコード手段とを有する記録媒体。

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

エンティティのＩＤベクトルの分割例を示す模式図である。

【図３】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図４】

記録媒体の実施例の構成を示す図である。

【符号の説明】

１　センタ

１ａ　秘密鍵生成器

１０，２０　メモリ

１１，２１　成分選出器

１２，２２　共通鍵生成器

１３　暗号化器

２３　復号器

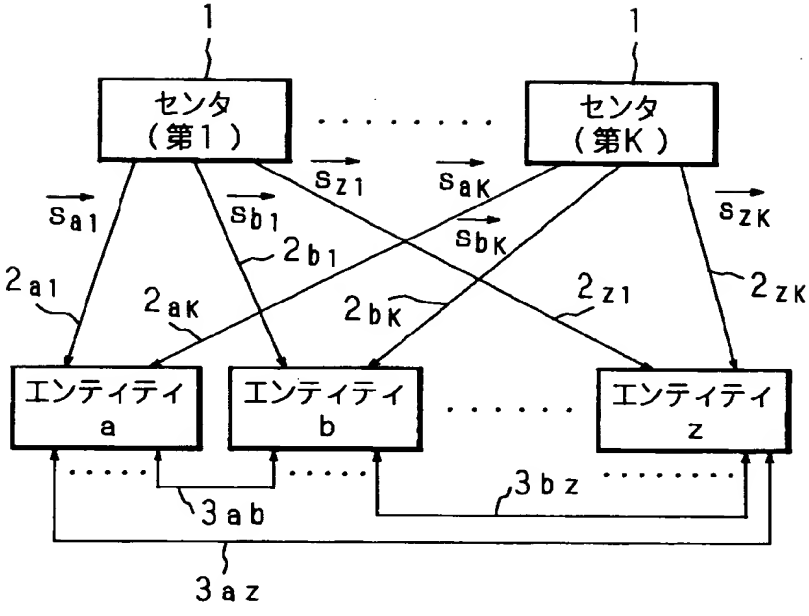
３０　通信路

４０　コンピュータ

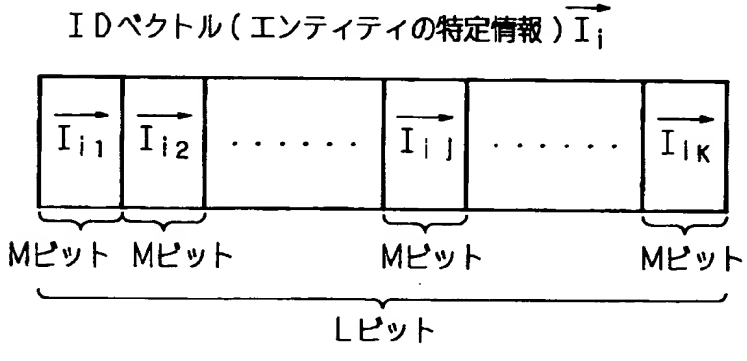
４１，４２，４３　記録媒体

【書類名】　　図面

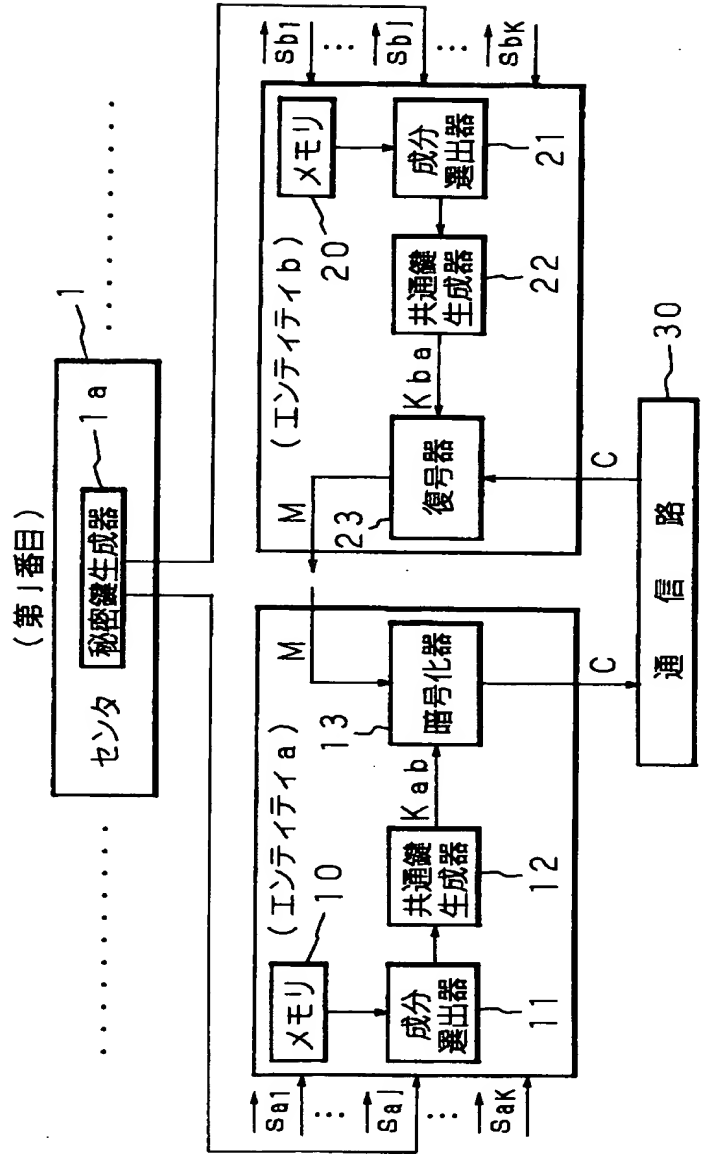
【図１】


1
1
センタ
（第1）
センタ
（第K）
$\overrightarrow{s_{z1}}$
$\overrightarrow{s_{aK}}$
$\overrightarrow{s_{a1}}$
$\overrightarrow{s_{b1}}$
$\overrightarrow{s_{bK}}$
$\overrightarrow{s_{zK}}$
2b1
2a1
2aK
2bK
2z1
2zK
エンティティ
a
エンティティ
b
エンティティ
z
3ab
3bz
3az

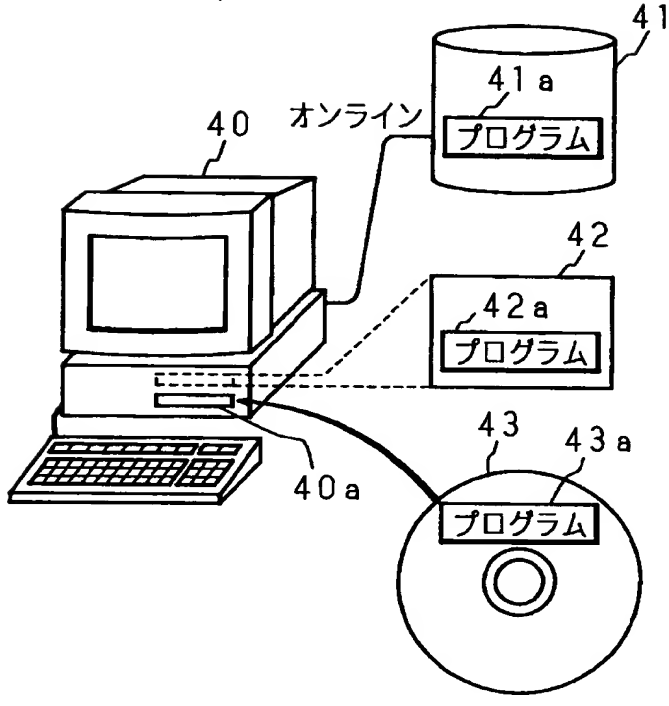
【図２】


IDベクトル（エンティティの特定情報）$\overrightarrow{I_i}$
$\overrightarrow{I_{i1}}$
$\overrightarrow{I_{i2}}$
$\overrightarrow{I_{ij}}$
$\overrightarrow{I_{iK}}$
Mビット
Mビット
Mビット
Mビット
Lビット

【図３】


（第ｉ番目）
センタ
秘密鍵生成器
1a
1
（エンティティａ）
10
メモリ
成分選出器
11
共通鍵生成器
12
Kab
暗号化器
13
M
C
（エンティティｂ）
20
メモリ
成分選出器
21
共通鍵生成器
22
Kba
復号器
23
M
C
通信路
30
Sa1
Sai
SaK
Sb1
Sbi
SbK

【図４】



【書類名】　　要約書

【要約】

【課題】　数学的構造を最小限に抑えて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる暗号通信方法を提供する。

【解決手段】　各エンティティへ固有の秘密鍵を配布するセンタ１が複数設けられており、各エンティティの特定情報（ＩＤ情報）をいくつかに分割し、その分割した特定情報毎に作成したすべての秘密鍵をエンティティに配布する。各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して共通鍵を生成する。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第０１６２５７号
受付番号	５９９０００５９６０７
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１１年　３月　８日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】　000006297
- 【住所又は居所】　京都府京都市南区吉祥院南落合町３番地
- 【氏名又は名称】　村田機械株式会社

【特許出願人】
- 【識別番号】　598159964
- 【住所又は居所】　東京都渋谷区神宮前四丁目２番１９号
- 【氏名又は名称】　辻井　重男

【特許出願人】
- 【識別番号】　597008636
- 【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号
- 【氏名又は名称】　笠原　正雄

【代理人】　申請人
- 【識別番号】　100078868
- 【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】　河野　登夫

次頁無

出願人履歴情報

識別番号　〔０００００６２９７〕

１．変更年月日　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出 願 人 履 歴 情 報

識別番号　〔５９７００８６３６〕

１．変更年月日　１９９７年　１月２１日
［変更理由］　新規登録
住　所　大阪府箕面市粟生外院４丁目１５番３号
氏　名　笠原　正雄

出 願 人 履 歴 情 報

識別番号　〔５９８１５９９６４〕

１．変更年月日　１９９８年１１月１９日
［変更理由］　新規登録
住　所　東京都渋谷区神宮前四丁目２番１９号
氏　名　辻井　重男